LA FRAUDE EN 3D

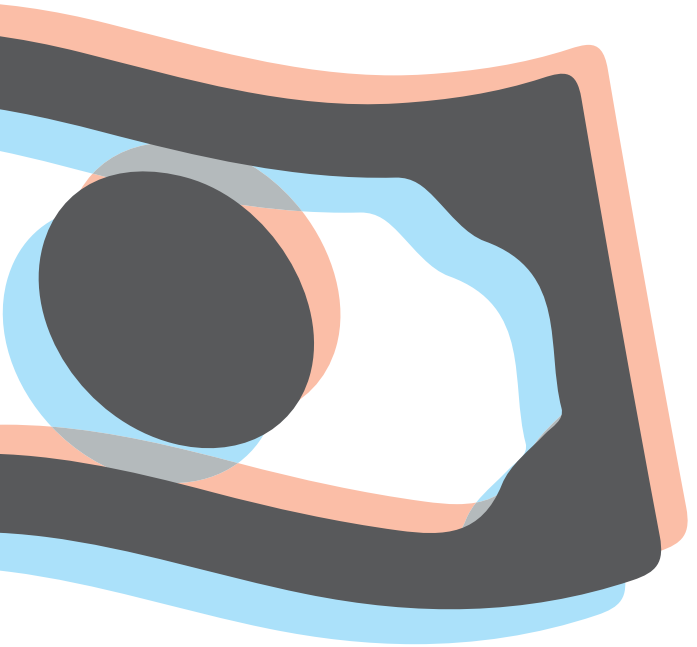
Détecter, Dénoncer, Décourager

Examiner chaque situation sous tous ses angles

Personne n'est à l'abri d'escroquerie, peu importe son âge, son niveau de scolarité ou son lieu de résidence.

La plupart des fraudes peuvent être évitées. C'est pourquoi il est important d'être vigilant et de les reconnaître afin de se protéger efficacement.

BANQUE DU CANADA
BANK OF CANADA



LA CONTREFAÇON DES BILLETS DE BANQUE

La vérification des billets de banque, c'est monnaie courante!

L'argent comptant est un moyen commode et rapide de payer ses achats. Comme il s'agit d'un mode de paiement utilisé par tous, celui-ci intéresse les faussaires. Chaque fois que vous acceptez un billet de banque sans le vérifier, vous risquez d'être victime de contrefaçon.

Que vous soyez caissier ou client, vous pouvez aider à empêcher les faux billets d'entrer en circulation. Les commerçants victimes de fraude subissent des pertes dont ils répercutent souvent le coût sur les consommateurs – en l'occurrence, vous!

Les billets de banque canadiens – en papier ou en polymère – sont pourvus d'éléments de sécurité qui sont faciles à vérifier et difficiles à contrefaire. Toutefois, les billets de banque ne sont sûrs que si vous les vérifiez. Si vous connaissez bien vos billets, vous pourrez détecter un faux en un coup d'œil.

Pour détecter une fausse coupure, il faut connaître les éléments de sécurité des billets. La vérification systématique **d'au moins deux éléments de sécurité** est la meilleure ligne de défense contre la contrefaçon. Comparez un billet douteux à un billet que vous savez authentique. Cherchez les différences et non les similitudes.

Comment vérifier les billets en polymère?

Touchez le billet, examinez-le et regardez au verso :

- Touchez la texture lisse et unique du billet. Celui-ci est fait d'un seul morceau de polymère dont certaines parties sont transparentes.
- Examinez le billet pour vérifier la présence de la bande transparente et du contour clair de la feuille d'érable givrée. De plus, examinez les détails du portrait et de l'édifice à reflets métalliques dans la bande transparente.
- Regardez au verso du billet pour vous assurer que les éléments dans la bande transparente ont les mêmes couleurs et détails qu'au recto.

Sachez qu'aucune loi ne vous oblige à accepter un billet de banque si vous doutez de son authenticité. Si on vous remet un billet d'une ancienne série avec lequel vous êtes moins familier, refusez-le et demandez qu'on vous remette un billet en polymère.

Voici ce que vous devez faire si vous pensez qu'on vous remet un faux billet au cours d'une transaction :

- Expliquez poliment que vous soupçonnez qu'il s'agit d'un faux billet.
- Demandez qu'on vous donne un autre billet (que vous vérifierez également).

- Conseillez à la personne d'apporter le billet suspect au service de police local pour le faire vérifier.
- Informez le service de police local qu'on a possiblement tenté de vous remettre un faux billet.

Si par mégarde vous avez en votre possession un billet suspect, remettez-le à votre service de police local pour le faire vérifier. S'il s'avère authentique, on vous le rendra.

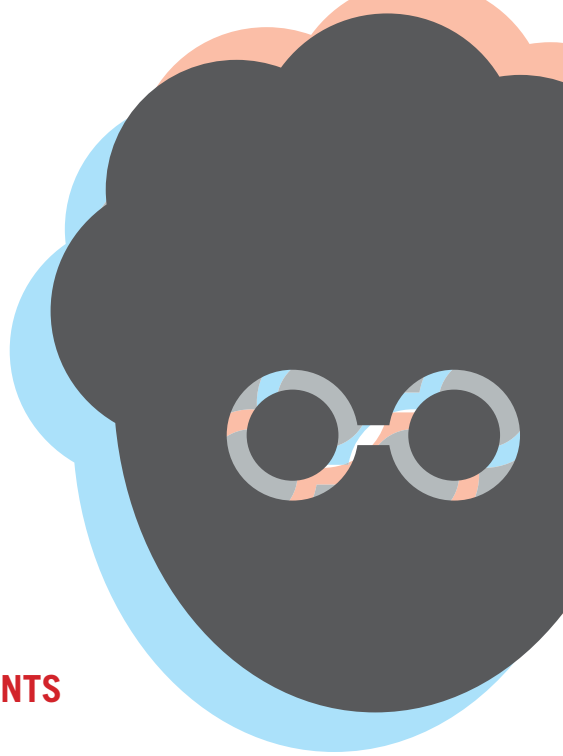
Comment vérifier les billets en papier

Pour en savoir davantage sur les éléments de sécurité des billets de banque canadiens, visitez le site www.banqueducanada.ca/billets/series-de-billets-de-banque/.

Si vous avez des doutes concernant un billet d'une ancienne série, demandez qu'on vous remette un billet en polymère (et vérifiez-le également).

Le billet commémoratif de 20 $ en polymère

Le 9 septembre 2015, la reine Elizabeth II est devenue le monarque au plus long règne de l'époque moderne au Canada. Pour souligner cet événement historique, la Banque a émis un billet commémoratif qui est une variante de l'actuel billet de 20 $ en polymère. Visitez le site www.banqueducanada.ca/billets/series-de-billets-de-banque/ pour connaître les éléments de sécurité de ce billet.



LA FRAUDE GRANDS-PARENTS

C'est quoi ?

Il s'agit d'une fraude par téléphone où des gens tenteront de se faire passer pour un membre de votre famille en situation de détresse invoquant un besoin urgent d'aide financière.

Comment font-ils ?

Les fraudeurs tentent généralement de se faire passer pour un membre de la famille (petits-enfants, nièce, cousin, ou même un ami d'un membre de la famille) qui est dans une situation d'urgence tel un accident ou une arrestation. Leur histoire suit généralement un scénario vraisemblable qui vise à déclencher des réactions d'anxiété et susciter un sentiment d'urgence d'agir.

Ils peuvent souvent invoquer qu'ils sont en compagnie de personnes en autorités comme un policier ou un professionnel tel qu'un médecin ou un avocat.

Ils réclament une aide financière d'urgence, notamment pour payer des dommages sur un véhicule, des honoraires, des frais de caution pour libération, des frais de soins, etc. Ils vous imploreront de ne pas en parler à leurs parents ou personne d'autre et même parfois de mentir sur la raison de votre retrait d'argent.

Certains fraudeurs pourront demander un virement d'argent tandis que d'autres vont envoyer quelqu'un à votre domicile pour récupérer la somme.

Comment se protéger

Voici quelques règles simples pour vous protéger et éviter d'être victime de ce type d'escroquerie:

- Les fraudeurs misent sur le fait que vous réagirez émotivement pour aider votre proche en situation d'urgence. Ils peuvent parfois être très insistants et multiplier les appels afin de générer davantage d'anxiété de votre part. Résistez à la pression et à l'envie d'agir rapidement.
- Ne donnez pas de renseignements personnels à votre interlocuteur.
- Posez des questions personnelles auxquelles seul votre proche serait en mesure de répondre.
- Appelez les parents, un autre membre de la famille ou des amis de la personne afin de vérifier la validité de l'histoire qui vous a été présentée.
- N'envoyez jamais d'argent à quelqu'un que vous ne connaissez pas et ne fournissez jamais votre numéro de carte de crédit à moins d'avoir validé l'identité de la personne avec laquelle vous transigez.
- Les policiers ne communiquent jamais avec des citoyens pour obtenir le versement d'une caution et n'ont jamais recours à un service de virement d'argent. En cas de doute et avant d'envoyer toute somme d'argent, communiquer avec le service de police qui dessert votre municipalité (Sûreté du Québec ou service de police local).

Si vous croyez avoir été victime de ce genre de fraude, portez plainte auprès du service de police qui dessert votre municipalité (Sûreté du Québec ou service de police local) et signalez le cas au Centre antifraude du Canada (1-888-495-8501).

FRAUDES SUR INTERNET

De quoi s'agit-il?

Qu'il s'agisse de gains financiers, de produit ou service miracle ou même de sentiment amoureux, les différentes approches autrefois utilisées par les fraudeurs sont toujours d'actualité et se sont adaptées au monde virtuel. Les mises en scène peuvent provenir de n'importe où dans le monde, par courriel, des sites Web et, souvent des deux à la fois.

Comment font-ils?

Les fraudeurs misent sur la méconnaissance et la vulnérabilité des gens et ont recours à une panoplie de moyens afin de mettre la main sur vos données personnelles. Ils peuvent :

- vous inciter à installer une application ou télécharger un logiciel malveillant qui peuvent endommager votre ordinateur de même que voler vos renseignements personnels ou financiers;
- utiliser la connexion Bluetooth dont sont équipés la plupart des appareils mobiles et ordinateurs portables pour s'introduire dans ceux-ci;
- vous envoyer des messages non sollicités par courriel ou messagerie instantanée dans le but de vous soutirer des informations confidentielles;

- créer des sites Web imitant des sites légitimes tels que des sites bancaires, des sites commerciaux et même des sites de réseaux sociaux afin de recueillir vos renseignements personnels;
- vous annoncer par courriel que vous avez gagné un prix ou que vous avez un héritage inattendu mais que, pour avoir accès à ce prix ou cette somme, vous devez d'abord payer des frais quelconques;
- faire appel à votre compassion et à vos sentiments amoureux pour obtenir de l'argent sous divers prétextes (frais de voyage, droits d'immigration, enfant malade, besoin de nourriture). Ils peuvent également tenter d'obtenir des photos intimes pour vous extorquer de l'argent par la suite.

Comment se protéger

Faites preuve de prudence et de scepticisme.

- **Utilisez des mots de passe difficiles à percer** composés de lettres majuscules, minuscules, de chiffres et de caractères spéciaux et dont la longueur devrait être au minimum de 8 caractères. N'utilisez pas le nom de votre animal de compagnie ou la date de naissance de votre enfant : ceux-ci peuvent être facilement déchiffrés.
- **Protégez votre ordinateur** à l'aide d'un pare-feu, d'un logiciel anti-virus et d'un programme anti-espions, et assurez-vous de les maintenir à jour.
- **Soyez prudent lorsque vous utilisez les médias sociaux** : vérifiez les paramètres de confidentialité et de sécurité des sites que vous fréquentez et soyez prudent avec l'information que vous y affichez.
- **Méfiez-vous des logiciels ou applications gratuits**, prenez toujours connaissance du contenu des licences d'exploitation et de la politique de confidentialité avant de les installer afin d'éviter de donner un accès pratiquement illimité à vos informations personnelles.

- **Protégez vos données**, chiffrez vos documents de nature délicate, faites des sauvegardes régulières de toutes vos données importantes. Prenez soin de verrouiller votre ordinateur et vos appareils mobiles lorsque vous ne les utilisez pas.
- **Protégez votre réseau sans fil** (Wi-Fi) à la maison car il peut être vulnérable aux intrusions. Les réseaux Wi-Fi publics sont également vulnérables. Évitez de faire des transactions financières ou des achats sur ces réseaux.
- **Recherchez le symbole** du cadenas sur le site Web ou le préfixe « https:// » au début de l'adresse du site (le « s » signifie « sécurisé ») pour vous assurer que le site est chiffré ou encodé lorsque vous devez transférer des informations personnelles ou financières, ou des mots de passe.
- **Interrogez-vous toujours** avant de cliquer sur un lien ou un fichier d'origine inconnue. Ne répondez jamais à des courriels où l'on vous demande de vérifier votre information ou encore de confirmer votre nom d'utilisateur ou votre mot de passe.

Si vous découvrez du contenu douteux sur Internet, si vous soupçonnez un délit informatique ou une fraude commerciale, si vous croyez avoir été victime de ce genre de fraude, portez plainte auprès du service de police qui dessert votre municipalité (Sûreté du Québec ou service de police local) et signalez le cas au Centre antifraude du Canada (1-888-495-8501).

LE VOL D'IDENTITÉ

C'est quoi ?

Le vol d'identité, ou usurpation d'identité, se produit lorsqu'une personne obtient et utilise, à votre insu et sans votre consentement, vos renseignements personnels à des fins criminelles. Les renseignements personnels comprennent toute information ou tout document servant à établir votre identité.

Les criminels peuvent utiliser vos renseignements pour :

- Accéder à vos comptes bancaires pour faire des achats et des retraits, allant même jusqu'à vous dérober toute votre épargne.
- Faire des demandes de prêts, de cartes de crédit, d'ouverture de comptes bancaires ou même obtenir un prêt hypothécaire.
- Obtenir un passeport ou toucher des prestations du gouvernement.

Comment font-ils ?

- En volant votre portefeuille, votre sac à main ou votre courrier résidentiel.
- En fouillant dans vos poubelles ou bac de recyclage pour récupérer vos factures, relevés bancaires et autres documents.
- En vous appelant et en se faisant passer pour votre créancier, votre propriétaire, votre employeur ou un enquêteur afin d'obtenir vos renseignements personnels.
- En envoyant des courriels non sollicités qui ressemblent à des courriels ou des sites légitimes (pourriels et hameçonnage).
- En écoutant vos conversations privées ou en regardant par-dessus votre épaule.
- En remplissant un formulaire de changement d'adresse pour rediriger votre courrier.
- En trafiquant des guichets automatiques et des terminaux de points de vente.
- En fouillant dans votre ordinateur, téléphone intelligent ou tablette et en regardant les courriels que vous avez envoyés.

Exemples de renseignements personnels :

- **nom complet**
- **date de naissance**
- **adresse**
- **adresse électronique**
- **numéro de téléphone**
- **mots de passe**
- **numéro d'assurance sociale (NAS)**
- **signature**
- **numéro de passeport**
- **numéro de permis de conduire**
- **données de cartes de crédit**

Comment se protéger ?

- Soyez particulièrement vigilant lorsque vous recevez des courriels, du courrier ou des appels spontanés où l'on vous demande des données personnelles ou financières. Ne donnez vos renseignements personnels que lorsque cela est absolument nécessaire et seulement lorsque vous avez confiance en la personne à qui vous vous adressez.
- Ne transmettez pas de renseignements personnels ou confidentiels par courriel ni par messagerie instantanée.
- Faites installer sur vos appareils électroniques (ordinateur, tablette et téléphone mobile) un antivirus, un filtre anti pourriel, un coupe-feu ainsi qu'un logiciel anti-espion pour réduire le risque de piratage informatique. Choisissez des mots de passe complexes et changez-les souvent.
- Déchiquetez vos reçus et relevés de carte de crédit, les offres de crédit pré-approuvées ou tout autre document contenant vos renseignements personnels avant d'en disposer.
- Vérifiez vos relevés de compte et de carte de crédit régulièrement. Contestez immédiatement tout achat qui vous est inconnu.
- Mémorisez vos mots de passe et vos numéros d'identification personnel (NIP) afin de ne pas en conserver de trace écrite. Lorsque vous composez votre NIP assurez-vous que personne autour de vous ne puisse le voir.
- Avant de partager vos renseignements personnels sur des réseaux sociaux, vérifiez vos paramètres de sécurité et considérez attentivement ce que vous vous apprêtez à afficher. Considérez toute information affichée sur les réseaux sociaux comme étant de l'information publique. Si vous partagez des photos et des vidéos en ligne, songez à retirer les géomarques (marques de localisation) pour éviter que l'on sache où vous habitez ou travaillez. Si votre caméra numérique, votre téléphone cellulaire ou votre caméra vidéo possède la fonction de géomarquage automatique, vous pouvez la désactiver.
- Une fois par année, demandez une copie de votre dossier de crédit auprès de TransUnion ou d'Équifax et assurez-vous qu'il ne comporte aucune erreur.

Notez que votre numéro d'assurance sociale (NAS) est un numéro confidentiel qui n'est requis par la loi que pour déclarer des revenus lorsqu'une personne les tire d'un emploi ou d'un investissement. Même si de nombreuses entreprises peuvent vous demander votre NAS à d'autres fins, vous avez le droit de refuser dans de telles circonstances.

Si vous soupçonnez ou savez avoir été victime d'un vol ou d'une fraude d'identité, signaler l'incident auprès du service de police qui dessert votre municipalité (Sûreté du Québec ou service de police local) et communiquez rapidement avec votre institution financière et avec la compagnie émettrice de votre carte de crédit.

Assurez-vous également de communiquer avec les deux agences nationales d'évaluation du crédit et demander qu'un avis de fraude soit inscrit à votre dossier de crédit.

- Equifax Canada
  Numéro sans frais : 1-800-465-7166
- TransUnion Canada
  Numéro sans frais : 1-877-525-3823

Communiquez avec le Centre antifraude du Canada pour signaler la fraude : 1-888-495-8501

NOTES

NOTES

POUR OBTENIR DE L'AIDE OU SIGNALER UNE FRAUDE

Si vous croyez avoir été victime de fraude, communiquez avec votre service de police local.

Pour des informations sur la prévention de la contrefaçon de monnaie, communiquez avec la Banque du Canada, au 1-800-303-1282, ou visitez www.banqueducanada.ca/billets.

Pour connaître les éléments de sécurité sur les billets de banque américains, visitez le www.newmoney.gov.

Pour joindre la Sûreté du Québec :
310-4141, ou *4141 à partir d'un cellulaire

Pour joindre le Service de police de la Ville de Montréal :
514-280-2222 ou communiquez directement avec votre poste de quartier

Pour joindre le Service de police de l'agglomération de Longueuil :
450-463-7011

Pour signaler une fraude auprès du Centre antifraude du Canada :
1-888-495-8501

Si vous désirez signaler une fraude ou toute autre activité criminelle **de manière anonyme et confidentielle** :

Pour la région de Montréal, communiquez avec Info-Crime, au 514-393-1133, ou visitez www.infocrimemontreal.ca.

À l'extérieur de Montréal, communiquez avec Échec au crime, au 1-800-711-1800, ou visitez www.echecaucrime.com.

mars 2016